```
Set     Items   Descriptio
S1       1072   RANDOM (N) (SEQUENC? OR NUMBER? OR NUMERIC?)()GENERATOR?
S2    9847566   GENERATE? OR REPRODUCE? OR CREATE? OR PRODUCE? OR DEVELOP?
S3       3064   NONCE OR RANDOM()(SEQUENCE? OR NUMBER? OR NUMERIC)
S4     953225   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE OR ENCIP-
            HER? OR CODING OR CODED OR ENCOD?
S5    3699223   BUS OR BUSES OR PATHWAY OR CHANNEL
S6      20932   (SECRET OR PRIVATE OR CRYPTO?)()(KEY OR KEYS OR CODE?) OR -
            PKI
S7         48   (PORTION OR PART OR SECTION)(3N)((DATA OR INFORMATION OR F-
            ACT?)()(SEGMENT? OR PIECE? OR BLOCK? OR CHUNK? OR BITS OR BYT-
            ES))
S8    2709752   DISTRIBUTION OR ALLOCATION OR DISSEMINATION OR DISPERSAL OR
             DISPERSION OR DISTRIBUTE?
S9      28691   (DEVICE? OR CLIENT? OR PC OR COMPUTER? OR WORKSTATION? OR -
            WORK()STATION? OR NODE? OR TERMINAL? OR PROCESSOR)(2N)(KEY OR
            KEYS)
S10       391   S1 (S) S2 (S) S3
S11       549   S5 (S) S6
S12         0   S7 (S) ((KEY OR KEYS)(3N) S8)
S13         0   S10 (S) S11 (S) S12 (S) S9
S14         0   S10 (S) S11
S15       117   S10 (S) (KEY OR KEYS)
S16         0   S10 (S) S11
S17         0   S7 (S) S8 (S) S9
S18         0   S7 (S) S8 (S) (KEY OR KEYS)
File 647:CMP  Computer Fulltext 1988-2004/Mar W3
        (c) 2004 CMP Media, LLC
File 275:Gale Group Computer DB(TM) 1983-2004/Apr 02
        (c) 2004 The Gale Group
File 674:Computer News Fulltext 1989-2004/Mar W3
        (c) 2004 IDG Communications
File 696:DIALOG Telecom. Newsletters 1995-2004/Apr 02
        (c) 2004 The Dialog Corp.
File 624:McGraw-Hill Publications 1985-2004/Apr 01
        (c) 2004 McGraw-Hill Co. Inc
File 636:Gale Group Newsletter DB(TM) 1987-2004/Apr 02
        (c) 2004 The Gale Group
File 813:PR Newswire 1987-1999/Apr 30
        (c) 1999 PR Newswire Association Inc
File 613:PR Newswire 1999-2004/Apr 02
        (c) 2004 PR Newswire Association Inc
File  16:Gale Group PROMT(R) 1990-2004/Apr 02
        (c) 2004 The Gale Group
File 160:Gale Group PROMT(R) 1972-1989
        (c) 1999 The Gale Group
File 553:Wilson Bus. Abs. FullText 1982-2004/Mar
        (c) 2004 The HW Wilson Co
```

4/22/04

```
Set     Items   Description
S1       3818   RANDOM (N) (SEQUENC? OR NUMBER? OR NUMERIC?)()GENERATOR?
S2    1154098   GENERATE? OR REPRODUCE? OR CREATE? OR PRODUCE? OR DEVELOP?
S3      13444   NONCE OR RANDOM()(SEQUENCE? OR NUMBER? OR NUMERIC)
S4     298669   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE OR ENCIP-
             HER? OR CODING OR CODED OR ENCOD?
S5     349702   BUS OR BUSES OR PATHWAY OR CHANNEL
S6       9337   (SECRET OR PRIVATE OR CRYPTO?)()(KEY OR KEYS OR CODE?) OR -
             PKI
S7       1229   (PORTION OR PART OR SECTION)(3N)((DATA OR INFORMATION OR F-
             ACT?)()(SEGMENT? OR PIECE? OR BLOCK? OR CHUNK? OR BITS OR BYT-
             ES))
S8     502550   DISTRIBUTION OR ALLOCATION OR DISSEMINATION OR DISPERSAL OR
              DISPERSION OR DISTRIBUTE?
S9      10699   (DEVICE? OR CLIENT? OR PC OR COMPUTER? OR WORKSTATION? OR -
             WORK()STATION? OR NODE? OR TERMINAL? OR PROCESSOR)(2N)(KEY OR
             KEYS)
S10      2492   S1 (S) S2 (S) S3
S11       976   S5 (S) S6
S12         3   S7 (S) ((KEY OR KEYS)(3N) S8)
S13         0   S10 (S) S11 (S) S12 (S) S9
S14        51   S10 (S) S9
S15         3   S14 (S) S11
S16       695   S10 (S) (KEY OR KEYS)
S17         0   S10 (S) S11 (S) S12 (S) S14 (S) S16
S18        18   S10 (S) S11
S19        51   S10 (S) S14
S20        18   S11 (S) S16
S21        50   S16 (S) S19
S22        69   S12 OR S14 OR S15 OR S18 OR S19 OR S20 OR S21
S23         6   S22 AND IC=(G11B? OR H04N?)
S24        50   S1 AND S2 AND NONCE
S25      3561   S1 AND S2 AND RANDOM()NUMBER
S26         1   ENCRYPTION()BUS()(KEY OR KEYS)
S27         3   ENCRYPTION(2N)BUS()(KEY OR KEYS)
S28       519   (PORTION OR PART OR SECTION)(3N)DATA()BLOCK?
S29       415   DEVICE()(KEY OR KEYS)
S30         0   S24 (S) S28
S31         3   S24 (S) S29
S32         2   S25 (S) S27
S33         6   S25 (S) S28
S34        31   S25 (S) S29
S35        12   S34 (S) S6
S36        20   S26 OR S27 OR S31 OR S32 OR S33 OR S35
S37        13   S36 NOT S22
S38         2   S37 AND IC=(G11B? OR H04N?)
File 348:EUROPEAN PATENTS 1978-2004/Mar W03
        (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040401,UT=20040325
        (c) 2004 WIPO/Univentio
```

38/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01329400
Encrypted data signal, data storage medium, data signal playback apparatus, and data signal recording apparatus
Verschlusseltes Datensignal, Speichermedium, Datensignal-Abspiel-Gerat und Datensignal-Speicher-Gerat
Signal de donnees crypte, support de donnees, appareil de reproduction de donnees et appareil d'enregistrement de donnees
PATENT ASSIGNEE:
MATSUSHITA ELECTRIC INDUSTRIAL CO., LTD., (216883), 1006, Oaza-Kadoma, Kadoma-shi, Osaka 571-8501, (JP), (Applicant designated States: all)
INVENTOR:
Nagai, Takahiro, 23-10-407, Takadono 6-chome, Asahi-ku, Osaka-shi, Osaka 535-0031, (JP)
Ishihara, Hideshi, 10-120, Ikuno 1-chome, Katano-shi, Osaka 576-0054, (JP)
Fukushima, Yoshihisa, 14-C-508, Sekime 6-chome, Joto-ku, Osaka-shi, Osaka 536-0008, (JP)
LEGAL REPRESENTATIVE:
Eisenfuhr, Speiser & Partner (100151), Martinistrasse 24, 28195 Bremen, (DE)
PATENT (CC, No, Kind, Date): EP 1134964 A2 010919 (Basic)
APPLICATION (CC, No, Date): EP 2001106146 010313;
PRIORITY (CC, No, Date): JP 200070020 000314
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: **H04N-001/00 ; H04N-001/32**

ABSTRACT EP 1134964 A2
Playing a data signal from an illegally produced data storage medium can be effectively disabled regardless of the type of storage medium so that copying can be prevented effectively at low cost. An encrypted data signal encrypting a copy-controlled data signal has superimposed thereto as a digital watermark identification data identifying the data signal as an encrypted signal. A data storage medium records this encrypted data signal, a data signal player reproduces the signal, and a data signal recorder records the signal.
ABSTRACT WORD COUNT: 83
NOTE:
Figure number on first page: 4

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 010919 A2 Published application without search report
LANGUAGE (Publication,Procedural,Application): English; English; English
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200138	1342
SPEC A	(English)	200138	10655
Total word count - document A			11997
Total word count - document B			0
Total word count - documents A + B			11997

INTERNATIONAL PATENT CLASS: **H04N-001/00 ...**

... H04N-001/32

...SPECIFICATION pass key for encrypting the data sent to the digital interface is also shared. Using this shared **bus key** , the **encryption** unit 614 of the PC encoder encrypts the data requiring protection (including key data and signal data...pass key for encrypting the data sent to the digital interface is also shared. Using this shared **bus key** , the **encryption** unit 914 of the PC drive 900-2 encrypts data requiring protection (such as the key data...

38/5,K/2 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00998015 **Image available**

METHOD AND APPARATUS FOR CONTENT PROTECTION ACROSS AN INTERFACE
PROCEDE ET APPAREIL DE PROTECTION DE CONTENU A TRAVERS UNE INTERFACE

Patent Applicant/Assignee:
INTEL CORPORATION, (a delawere Corporation), 2200 Mission College Boulevard, Santa Clara, CA 95052, US, US (Residence), US (Nationality)
Inventor(s):
TRAW Brendan, 10859 NW Supreme Court, Portland, OR 97229, US,
RIPLEY Mike, 1222 NE 56th Court, Hillsboro, OR 97124, US,
Legal Representative:
MALLIE Michael J (et al) (agent), Blakely Sokoloff Taylor & Zafman, 12400 Wilshire Boulevard, 7th Floor, Los Angeles, CA 90025, US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200328026 A1 20030403 (WO 0328026)
Application: WO 2002US17961 20020606 (PCT/WO US0217961)
Priority Application: US 2001960786 20010922
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G11B-020/00**
International Patent Class: **H04N-007/24** ; **H04N-007/167**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5184

English Abstract
A method and apparatus to protect unencrypted content or data in a storage media from prohibited use or reproduction by encrypting unprotected content before it is transmitted to another device or software application. A compliant device or software application is capable of decrypting the content, detecting any watermark within the content, and accessing or processing the content according to the restrictions associated with the detected watermark. Non-compliant devices or software are prevented from accessing or processing the content since they are unable to decrypt it.

French Abstract
L'invention concerne un procede et un appareil de protection de contenu ou de donnees non cryptes dans un support de stockage contre l'utilisation ou la reproduction prohibees par le cryptage de contenu non protege avant qu'il ne soit transmis vers un autre dispositif ou une autre application logicielle. Un dispositif ou une application logicielle flexibles peuvent decrypter le contenu, detecter n'importe quel filigrane dans le contenu, et acceder a ou traiter le contenu en fonction des restrictions associees au filigrane detecte. Il est possible d'empecher des dispositifs ou des logiciels non flexibles d'avoir acces a ou de traiter le contenu puisqu'ils sont incapables de le decrypter.

Legal Status (Type, Date, Text)
Publication 20030403 A1 With international search report.
Examination 20030626 Request for preliminary examination prior to end of 19th month from priority date

Main International Patent Class: **G11B-020/00**
International Patent Class: **H04N-007/24** ...

... **H04N-007/167**
Fulltext Availability:
Detailed Description

Detailed Description
... key.

According to one implementation of the encryption/decryption scheme for this content copy protection system, a **random number generator** on the destination device 404 **generates** a random or sequential number (referred hereinafter as "nonce") and ...a previously calculated media key using a one-way function and returns the result (i.e., a **bus key**) to an **encryption** logic component in the source device 402. The one-way function is configured such that the bus key can be **generated** by inputting the media key and the nonce, however, determining the media key from the bus key the previously calculated media key and the nonce to **produce** its own bus key to be used by a decryption logic component in the destination device 404...

...source
11
device 402 and destination device 404, both source and destination devices 402 and 404 will **generate** the same bus key provided that same media key and nonce was used by both devices to **generate** the bus key. In this manner, content from the storage media may be protected during transmission.

After...

```
Set     Items   Description
S1       3818   RANDOM (N) (SEQUENC? OR NUMBER? OR NUMERIC?)()GENERATOR?
S2    1154098   GENERATE? OR REPRODUCE? OR CREATE? OR PRODUCE? OR DEVELOP?
S3      13444   NONCE OR RANDOM()(SEQUENCE? OR NUMBER? OR NUMERIC)
S4     298669   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE OR ENCIP-
             HER? OR CODING OR CODED OR ENCOD?
S5     349702   BUS OR BUSES OR PATHWAY OR CHANNEL
S6       9337   (SECRET OR PRIVATE OR CRYPTO?)()(KEY OR KEYS OR CODE?) OR -
             PKI
S7       1229   (PORTION OR PART OR SECTION)(3N)((DATA OR INFORMATION OR F-
             ACT?)()(SEGMENT? OR PIECE? OR BLOCK? OR CHUNK? OR BITS OR BYT-
             ES))
S8     502550   DISTRIBUTION OR ALLOCATION OR DISSEMINATION OR DISPERSAL OR
              DISPERSION OR DISTRIBUTE?
S9      10699   (DEVICE? OR CLIENT? OR PC OR COMPUTER? OR WORKSTATION? OR -
             WORK()STATION? OR NODE? OR TERMINAL? OR PROCESSOR)(2N)(KEY OR
             KEYS)
S10      2492   S1 (S) S2 (S) S3
S11       976   S5 (S) S6
S12         3   S7 (S) ((KEY OR KEYS)(3N) S8)
S13         0   S10 (S) S11 (S) S12 (S) S9
S14        51   S10 (S) S9
S15         3   S14 (S) S11
S16       695   S10 (S) (KEY OR KEYS)
S17         0   S10 (S) S11 (S) S12 (S) S14 (S) S16
S18        18   S10 (S) S11
S19        51   S10 (S) S14
S20        18   S11 (S) S16
S21        50   S16 (S) S19
S22        69   S12 OR S14 OR S15 OR S18 OR S19 OR S20 OR S21
S23         6   S22 AND IC=(G11B? OR H04N?)
File 348:EUROPEAN PATENTS 1978-2004/Mar W03
         (c) 2004 European Patent Office
File 349:PCT FULLTEXT 1979-2002/UB=20040401,UT=20040325
         (c) 2004 WIPO/Univentio
```

23/5,K/1 (Item 1 from file: 348)
DIALOG(R)File 348:EUROPEAN PATENTS

01449329

APPARATUS AND METHOD FOR RECORDING/REPRODUCING INFORMATION
VORRICHTUNG UND VERFAHREN ZUR AUFZEICHNUNG/WIEDERGABE VON INFORMATIONEN
APPAREIL ET PROCEDE PERMETTANT D'ENREGISTRER ET DE REPRODUIRE DES INFORMATIONS

PATENT ASSIGNEE:
Sony Corporation, (214028), 7-35, Kitashinagawa 6-chome, Shinagawa-ku, Tokyo 141-0001, (JP), (Applicant designated States: all)
INVENTOR:
TAKI, Ryuta, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shigawa-ku, Tokyo 141-0001, (JP)
ASANO, Tomoyuki, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shinagawa-ku, Tokyo 141-0001, (JP)
OISHI, Tateo, c/o SONY CORPORATION, 7-35, Kitashinagawa 6-Chome, Shinagawa-ku, Tokyo 141-0001, (JP)
OSAWA, Yoshitomo, c/o SONY CORPORATION, 7-35, KITAShinagawa 6-Chome, Shinagawa-ku, Tokyo 141-0001, (JP)
LEGAL REPRESENTATIVE:
Turner, James Arthur et al (74631), D. Young & Co., 21 New Fetter Lane, London EC4A 1DA, (GB)

PATENT (CC, No, Kind, Date): EP 1265396 A1 021211 (Basic)
WO 2002056535 020718
APPLICATION (CC, No, Date): EP 2002729546 020111; WO 2002JP119 020111
PRIORITY (CC, No, Date): JP 20017238 010116
DESIGNATED STATES: AT; BE; CH; CY; DE; DK; ES; FI; FR; GB; GR; IE; IT; LI; LU; MC; NL; PT; SE; TR
EXTENDED DESIGNATED STATES: AL; LT; LV; MK; RO; SI
INTERNATIONAL PATENT CLASS: H04L-009/00; G06F-012/14; **G11B-027/00** ; **G11B-020/10**

ABSTRACT EP 1265396 A1
A system and method are realized which enables valid use of content by preventing unauthorized use of content which is caused by rewriting rights data. A structure is employed in which rights data including use-restriction information on content and DRM data including an encrypted content key are recorded in a digital data recording medium (media), and in which an integrity check value (ICV) for the DRM data can be stored in a recordable/playable area (protected area) by using only a dedicated IC. EKB distribution is used to execute the tree-structure key distribution to distribute keys for generating ICV-generation verifying keys. In this structure, unauthorized use of content by rewriting of the rights data is prevented.
ABSTRACT WORD COUNT: 116
NOTE:
Figure number on first page: 0018

LEGAL STATUS (Type, Pub Date, Kind, Text):
Application: 020911 A1 International application. (Art. 158(1))
Application: 020911 A1 International application entering European phase
Application: 021211 A1 Published application with search report
Examination: 021211 A1 Date of request for examination: 20020902
LANGUAGE (Publication,Procedural,Application): English; English; Japanese
FULLTEXT AVAILABILITY:

Available Text	Language	Update	Word Count
CLAIMS A	(English)	200250	4124
SPEC A	(English)	200250	23236
Total word count - document A			27360
Total word count - document B			0
Total word count - documents A + B			27360

...INTERNATIONAL PATENT CLASS: **G11B-027/00** ...

... G11B-020/10
...SPECIFICATION processing flow in Fig. 15.

First, by using the key generator 2 or 621 such as a **random number generator** , the ICV **key** is **generated** (S201). Next, by using a **key** set (a leaf **key** and a **node key**) that the **device** possesses, the EKB processor (Process EKB) 614 executes the process for decrypting the EKB. When acquisition of the EKB **key** is a success (Yes in S202), the process proceeds to step S203. When the device has been revoked, etc., it is impossible to acquire the EKB **key** by decrypting the EKB (No in step S202), the process ends.

Next, by using the EKB key...case of updating the DRM data is described using the processing block diagram in Fig. 24. The **device** uses a **key** generator 1122 such as a **random number generator** to **generates** the ICV **key** , and **generates** the ICV-generation verifying **key** by using the EKB **key** to act on the ICV **key** in the **key** generator (Func) 1122.

In addition, by using an ICV generating means (Calculate) 1123 to execute the ICV...

23/5,K/2 (Item 1 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00946951 **Image available**

METHOD AND SYSTEM FOR PROVIDING BUS ENCRYPTION BASED ON CRYPTOGRAPHIC KEY EXCHANGE

PROCEDE ET SYSTEME POUR ASSURER LE CHIFFREMENT D'UN BUS SUR LA BASE D'ECHANGE DE CLES CRYPTOGRAPHIQUES

Patent Applicant/Assignee:
INTEL CORPORATION, 2200 Mission College Boulevard, Santa Clara, CA 95052, US, US (Residence), US (Nationality)
Inventor(s):
TRAW Brendan, 10859 NW Supreme Court, Portland, OR 97229, US,
RIPLEY Mike, 1222 NE 56th Court, Hillsboro, OR 97124, US,
Legal Representative:
MALLIE Michael J (agent), Blakely, Sokoloff, Taylor & Zafman, 7th Floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (et al), US,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200280170 A2-A3 20021010 (WO 0280170)
Application: WO 2002US7085 20020307 (PCT/WO US0207085)
Priority Application: US 2001823423 20010329
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZM ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: **G11B-020/00**
International Patent Class: **H04N-007/167**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 5035

English Abstract
A system is described for protecting digital content stored (112) on a storage medium (108) from unauthorized copying. The system includes a number generator to generate a nonce, an encryption subsystem (114) and a decryption subsystem (128). The encryption subsystem encrypts data accessed from a storage medium containing a key distribution data block (MKB,110) using an encryption bus key (124) prior to transmitting the encrypted data via a data bus (106). The encryption bus key is derived

based on at least a portion of the key distribution data block (110), at least one device key (116) assigned to the encryption subsystem and the nonce generated by the number generator. The decryption subsystem is coupled to the data bus to decrypt the encrypted data received over the data bus using a decryption bus key (140) derived based on at least a portion of the key distribution data block, at least one device key (130) assigned to the decryption subsystem and the nonce generated by the number generator.

French Abstract

L'invention porte sur un systeme de protection d'un contenu numerique stocke dans une memoire a partir d'une copie non autorisee. Le systeme comprend un generateur de nombres destine a generer un intervalle de confiance, un sous-systeme de chiffrement et un sous-systeme de dechiffrement. Le sous-systeme de chiffrement chiffre des donnees d'un support d'enregistrement contenant un bloc de donnees de distribution de cles utilisant une cle de bus de chiffrement avant de transmettre les donnee chiffrees par un bus. La cle du bus de chiffrement est derivee sur la base d'au moins une partie du bloc de donnees de distribution de cles, au moins une cle de dispositif etant affectee au sous-systeme de chiffrement et l'intervalle de confiance genere par le generateur de nombres. Le sous-systeme de dechiffrement est couple au bus de donnees afin de dechiffrer les donnees chiffrees recues sur le bus de donnees au moyen d'une cle de bus de dechiffrement derivee sur la base d'au moins une partie du bloc de donnees de distribution de cles, au moins une cle du dispositif affectee au sous-systeme de dechiffrement et l'intervalle de confiance genere par le generateur de nombres.

Legal Status (Type, Date, Text)

Publication	20021010	A2 Without international search report and to be republished upon receipt of that report.
Examination	20030109	Request for preliminary examination prior to end of 19th month from priority date
Search Rpt	20030605	Late publication of international search report
Republication	20030605	A3 With international search report.

Main International Patent Class: **G11B-020/00**
International Patent Class: **H04N-007/167**
Fulltext Availability:
Claims

Claim

... generator is a random
number generator residing within said decryption subsystem.
12
. A method comprising:
a storage **device** reading a **key** distribution data block from a storage medium;
the storage device processing at least a portion of said **key** distribution data
block using at least one **device** **key** to compute a media **key** ;
the storage **device** fetching a **nonce** **generated** by a number generator;
the storage device combining said **nonce** with said media **key** using a one
way function to **generate** a bus **key** ;
the storage **device** encrypting data read from the storage medium using the
I 0 bus **key** **generated** by the storage device; and
the storage device transmitting the encrypted data over a data bus.

12...

23/5,K/3 **(Item 2 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00891492 **Image available**

OPTICAL DISC AND A REPRODUCTION METHOD, REPRODUCTION APPARATUS, AND RECORDING APPARATUS FOR THE SAME

DISQUE OPTIQUE ET PROCEDE DE REPRODUCTION, APPAREIL DE REPRODUCTION, ET APPAREIL D'ENREGISTREMENT ASSOCIE

Patent Applicant/Assignee:
MATSUSHITA ELECTRIC INDUSTRIAL CO LTD, 1006, Oaza Kadoma, Kadoma-shi, Osaka 571-8501, JP, JP (Residence), JP (Nationality), (For all designated states except: US)

Patent Applicant/Inventor:
SHOJI Mamoru, 3-13-4-805, Mozuumemachi, Sakai-shi, Osaka 591-8032, JP, JP (Residence), JP (Nationality), (Designated only for: US)
NAKAMURA Atsushi, Syokoryo, 25-3, Mido-cho, Kadoma-shi, Osaka 571-0064, JP, JP (Residence), JP (Nationality), (Designated only for: US)
ISHIDA Takashi, 13-14, Hashimoto-Isoku, Yawata-shi, Kyoto 614-8331, JP, JP (Residence), JP (Nationality), (Designated only for: US)
ISHIBASHI Hiromichi, 6-H-503, Tenno 2-chome, Ibaraki-shi, Osaka 567-0876, JP, JP (Residence), JP (Nationality), (Designated only for: US)
MIYASHITA Harumitsu, B101, 5-15, Niina, Minoo-shi, Osaka 562-0005, JP, JP (Residence), JP (Nationality), (Designated only for: US)
SENGA Hisashi, 3-14-527, Miyukihigashimachi, Neyagawa-shi, Osaka 572-0055, JP, JP (Residence), JP (Nationality), (Designated only for: US)
TAKAHASHI Rie, 7-85, Ikagakitamachi, Hirakata-shi, Osaka 573-0036, JP, JP (Residence), JP (Nationality), (Designated only for: US)

Legal Representative:
AOYAMA Tamotsu (et al) (agent), AOYAMA & PARTNERS, IMP Building, 3-7, Shiromi 1-chome, Chuo-ku, Osaka-shi, Osaka 540-0001, JP,

Patent and Priority Information (Country, Number, Date):
Patent: WO 200225645 A2-A3 20020328 (WO 0225645)
Application: WO 2001JP8267 20010921 (PCT/WO JP0108267)
Priority Application: JP 2000288346 20000922; JP 2000292034 20000926; JP 2000323676 20001024

Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS KE KG KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PH PL PT RO RU SD SE SG SI SK SL TJ TM TR TT TZ UA UG US UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GQ GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM

Main International Patent Class: **G11B-007/013**
International Patent Class: **G11B-020/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 29044

English Abstract
An optical disk, and a method and apparatus for reproducing and/or recording data to the disk are provided for preventing illegal copying of authorized disks recording copyrighted digital content. The optical disk 10 has a control area 12 for storing control data, a data area 14 for storing main digital data (content), and an identification area 13 for storing sub-digital data specific to the main digital data. The sub-digital data is recorded as a pit sequence (R1, R3, R5) at a locally phase modulated clock timing. When disk identification data is recorded as the sub-digital data, key information stored to the reproduction apparatus is compared with identification data (sub-digital data) detected from jitter fluctuations in the identification area 13 when content is reproduced from the optical disk 10. If a specific correlation is thus confirmed, the disk is recognized as a legally copied disk and reproduction is enabled. Illegal copies can thus be prevented.

French Abstract
L'invention concerne un disque optique, ainsi qu'un procede et un

appareil permettant de reproduire et/ou d'enregistrer des donnees sur ledit disque de maniere a empecher la copie illegale de disques autorises enregistrant un contenu numerique protege. Le disque optique comporte une zone de controle (12) stockant des donnees de controle, une zone de donnees (14) stockant les donnees numeriques principales (le contenu) et une zone d'identification (13) stockant des donnees sous-numeriques specifiques aux donnees numeriques principales. Les donnees sous-numeriques sont enregistrees comme sequence a depression (R1, R3, R5) selon une synchronisation d'horloge a modulation de phase locale. Lorsque les donnees d'identification de disque sont enregistrees comme donnees sous-numeriques, les informations cle, stockees dans l'appareil de reproduction, sont comparees aux donnees d'identification (donnees sous-numeriques) detectees a partir de fluctuations de gigue dans la zone d'identification (13) lorsque le contenu est reproduit a partir du disque optique (10). Si une correlation particuliere est ainsi confirmee, le disque est reconnu comme etant un disque legalement copie et la reproduction est activee, ce qui permet d'empecher des copies illegales.

Legal Status (Type, Date, Text)
Publication 20020328 A2 Without international search report and to be republished upon receipt of that report.
Examination 20020822 Request for preliminary examination prior to end of 19th month from priority date
Search Rpt 20021128 Late publication of international search report
Republication 20021128 A3 With international search report.
Republication 20021128 A3 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

Main International Patent Class: **G11B-007/013**
International Patent Class: **G11B-020/00**
Fulltext Availability:
Detailed Description

Detailed Description
... initial value
memory 102b confidentially prestores the initial value for a pseudorandom number series generated by pseudo- **random number generator** 104.

The encryption key memory 102c stores the 56-bit encryption key input from the encryption section...

23/5,K/4 (Item 3 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00828328 **Image available**
SYSTEM AND METHOD FOR PROTECTING DATA STREAMS IN HARDWARE COMPONENTS
SYSTEME ET PROCEDE DE PROTECTION DES TRAINS DE DONNEES DANS DES COMPOSANTS MATERIELS
Patent Applicant/Assignee:
MICROSOFT CORPORATION, One Microsoft Way, Redmond, WA 98052, US, US (Residence), US (Nationality)
Inventor(s):
MALVAR Henrique, 2302 233rd Avenue N.E., Redmond, WA 98053, US,
ENGLAND Paul, 16659 Northrup Way, Bellevue, WA 98008, US,
Legal Representative:
LEE Lewis C (et al) (agent), 421 W. Riverside Avenue, Suite 500, Spokane, WA 99201, US,
Patent and Priority Information (Country, Number, Date):
Patent: WO 200161904 A1 20010823 (WO 0161904)
Application: WO 2001US1683 20010117 (PCT/WO US0101683)
Priority Application: US 2000507478 20000217
Designated States: AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CR CU CZ DE DK DM DZ EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ PL PT RO RU SD SE SG

SI SK SL TJ TM TR TT TZ UG UZ VN YU ZA ZW
(EP) AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE TR
(OA) BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
(AP) GH GM KE LS MW MZ SD SL SZ TZ UG ZW
(EA) AM AZ BY KG KZ MD RU TJ TM
Main International Patent Class: H04K-001/02
International Patent Class: **H04N-005/00**
Publication Language: English
Filing Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 7855

English Abstract
A scrambling architecture protects data streams in the operating system and hardware components of a computer by scrambling the otherwise raw data prior to the data being handled by the operating system. The architecture has a scrambler implemented at either the client or the server that adds noise to the content. More specifically, the scrambler produces periodic sets of tone patterns having varying amplitudes based on a first key. The scrambler also generates a random signal based on a first key and a second key. The tone patterns and random signal are added to the content to scramble the content. The scrambled content is then passed to the filter graph. The descrambler detects the tone patterns in the content and recovers the first key from the varying amplitudes of the tone patterns. The descrambler also receives the second key via a separate channel (e.g., a cryptographically secured path) and generates the same random signal using the recovered first key and the second key. The descrambler subtracts the tone patterns and the random signal from the scrambled content.

French Abstract
La presente invention concerne une architecture de brouillage protegeant les trains de donnees dans le systeme d'exploitation et les composants materiels d'un ordinateur. Il s'agit de brouiller des donnees brutes avant leur manipulation par le systeme d'exploitation. On dispose a cet effet au niveau du client ou du serveur d'un brouilleur ajoutant du bruit au contenu. De facon plus specifique, le brouilleur produit des ensembles periodiques de structures sonores dont les amplitudes varient sur la base d'une premiere cle. Le brouilleur produit egalement un signal aleatoire sur la base de la premiere cle et d'une seconde cle. Les structures sonores et le signal aleatoire ajoutes au contenu viennent le brouiller. Le contenu brouille est alors remis brouille pour traitement au graphe a filtre. Ce desembrouilleur recherche dans le contenu les structures sonores et reconstruit la premiere cle sur la base de leurs variations d'amplitude. Il recoit egalement la seconde cle via un canal separe, tel qu'un chemin securise par cryptographie, puis produit le meme signal aleatoire sur la base de la premiere cle retablie et de la seconde cle pour. Pour restituer le contenu, le desembrouilleur elimine du contenu brouille les structures sonores.

Legal Status (Type, Date, Text)
Publication 20010823 A1 With international search report.
Publication 20010823 A1 Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.
Examination 20011115 Request for preliminary examination prior to end of 19th month from priority date

International Patent Class: **H04N-005/00**
Fulltext Availability:
Claims

Claim
... client. For instance, a publisher will typically retain copyright to a work so that the client cannot **reproduce** or publish the work without

pen-nission. A publishe[redacted]ould also adjust pricing accor[redacted]g to whether the...

...certificates, and storing data securely. Fla. I shows a representative prior art system 20 having a content **producer** /provider 22 that **produces** original content (e.g., audio, video) and distributes the content over a network 24 to a client 26. The content **producer** /provider 22 has a content storage 30 to store digital data streams of original content and a...

...the source material by keeping an encrypted copy of the content on disk, and keeping a decryption **key** safely somewhere. While this architecture safely protects the content from the provider 22 to the client 26...

...technology from Microsoft Corporation. The
ZD ZD
mixer 64 processes the PCM data with other sources to **produce** a desired output. At ...noise by adding a random signal to the content. More particularly, the client has a scrambler to **produce** periodic sets of deterministic tone patterns. The scrambler modulates the amplitude of the tone patterns based on a first **key** , thereby embedding the first **key** into the modulated tone patterns. The scrambler also **generates** a random signal based on the first **key** and a second **key** . The tone patterns and random signal are added to the PCM data to scramble the content. The...

...subtracting out the noise. The descrambler detects the tone patterns in the content and recovers the first **key** from the varying amplitudes of the tone patterns. The descrambler also receives the second **key** via a separate **channel** (e.g., a cryptographically secured path) and **generates** the same random signal based on the recovered first **key** and the second **key** . The descrambler subtracts the tone patterns and the random signal from the scrambled content to restore the...

...and playback content. The tamper-resistant software stops attackers from easily modifying this
:D
component or extracting **keys** . However, at some point the audio must be handed to the operating system for playback. The architecture...

...to the media output device(s) 44. The scrambler 106 and descrambler 112 utilize one or more **secret keys** 114 to **generate** the scrambling signal that is added to the PCM data. The **keys** 1 14 may be passed between the media player 102 and the driver II 0 through an in-band **channel** accompanying the scrambled data, and/or via an out-of-band **channel** separate from the data path (e.g. the IOCTL device 1/0 control **channel** in DirectX). One implementation of the media player 102 and driver I 10, and the **keys** utilized to scramble and unscramble PCM data, is described below in more detail with reference to Fig...

...incentive for the theft. Moreover, it is very difficult to unscramble the data without knowledge of the **keys** 1 14.
Scrambfin2 Techniques
There are different ways to implement the scrambling architecture at the client to...

...is to add noise to the signal. In the audio context, one noise-addition scheme is to **generate** a set of speech, music or noise-like functions using a session **key** and add those functions to the signal, either directly in the time domain or in a frequency...

...domain. The choice of function, its amplitude, phase, and dilation is selected on the basis of the **key** generator. Addiner a few tens of noise bursts per second renders the signal noise is quite large, even if the attacker knows the noise basis. However, given the **key** (and assuming no overloads) the noise signal can be subtracted exactly to return to the unscrambled state...
...segments. Within each frame, segments are permuted and reassembled.

Typically, each frame uses a different permutation. A **secret key** controls the sequence of permutations. In frequency-domain scrambling, the signal is partitioned into overlapping frames (e...

...filter bank. The frequency bands are pen-nuted and sent through a svnthesis filter bank. Again, a **secret key** controls the sequence of permutations. Frequencydomain scrambling is harder to break than time-domain scrambling, but has...

...to the data (step 206). The scrambler 106 has a tone burst generator and modulator 120 to **generate** a synchronization tone and a cryptographic pseudo **random number generator** (PRNG) 122 to **generate** a random signal. Both the syne tone and the random signal are added to the PCM data to **produce** noisy or scrambled PCM data. The tone burst generator 120 and PRNG 122 use two levels of **keys** to **create** the sync tone and random signal: (1) an "in-band" **key** 124, and (2) an "out-ofband" or "session" **key** 126. Both the tone burst generator 120 and the PRNG 122 use the in-band **key** 124, while only the PRNG 122 uses the out-of-band **key** 126. The **keys** may be implemented, for example, with large bit length, such as 56-bit or 128-bit **keys** . The tone burst generator and modulator 120 uses the in-band **key** to **generate** sets of tone bursts that can be easily recognized at the descrambler (step 208 in Fig. 5...

...304 utilizes +0 0.5 to represent a second binary value (e.g., 0). The in-band **key** 124 is embedded into the sets of tone burst sequences as an aggregate of the bits in order to pass the **key** along with the data to the driver. The in-band **key** can be changed with each audio/video clip, with sets of clips, or even within clips. The kHz, the tone burst generator 120 **generates** a synchronization tone at 22.05 kHz. The tone can be easily detected at the descrambler and...

...will remove this tone frequency.
With reference again to Figs. 4 and 5, the cryptographic PRNG 122 **generates** a pseudo random signal using the in-band **key** and the out-of-band session **key** (step 210 in Fig. 5). Fig. 7 shows an exemplary **random sequence** 400 having a
random pattern of data values with amplitudes of +1 or The PRNG 122 is...

...being zero to avoid introducing a DC shift to the original data signal. While the in-band **key** 124 is embedded into the tone sync signal, the session **key** 126 is kept independent of the data and passed over a separate **channel** 128 1 5 from the data path. The session **key** 126 is protected using a **cryptographic key** exchange (e.g., a Diffie-Hellman exchange and authentication) to ensure that the **key** 126 is safely transported from the media player 102 to the driver I 10 over the **channel** 128 (which can be the IOCTL device control **channel** in DirectX, for example). Accordingly, the scrambler 106 or media player 102 is equipped with encryption and signing capabilities to encrypt and sign the session **key** for secure transportation to the driver 1 1 0 and descrambler 1 12.
The scrambler 106 adds...

...and delay introduced by the filter graph 108, and demodulates the tones to recover the in-band **key** 124 (step 218 in Fig. 5). The tone detector 140 passes the recovered in-band **key** 124 to the PRNG 142. The descrambler 112 also receives the session **key** 126 from the out-of-band **channel** 128, decrypts and authenticates it, and gives the **key** 126 to the PRNG 142. The descrambler is equipped with decryption and verification means to decrypt and authenticate the session **key** as having been sent from the media player 102. The PRNG 142 implements the same algorithm as that used in the media driver's PRNG 122. Given the same in-band **key** 124 and session **key** 126, the PRNG 142 recreates the same random signal that was previously added to the PCM data...

...energy after tone subtraction is minimized. The regenerated sync tone with the correct gain and delay is **produced** in module 5'1 0.
Detection of the in-band **key** is performed by amplitude demodulation

module 512. For each tone burst, the module compares the burst amplitude ...amplitude is equal to 1.0 and the averacre is 0.75), then a bit of the **key** is demodulated as having one binary value (say "one"). If the amplitude is below that average (say...

...amplitude is equal to 0.5 and the average is 0.75), then a bit of the **key** is demodulated as having the other binary value (say "zero"). The process is repeated for subsequent tone burst until all bits of the in band **key** 124 are recovered. The in-band **key** 124 can then be used by the
cryptographic PRNG 142 to regenerate the random noise sequence to...

...may be scrambled by XORing at least a portion of the content with a random bit stream **generated** by the PRNG 122. For instance, for 16 bit audio, the least significant 13 bits are XORed with bits **generated** by the PRNG 122. This effectively scrambles the content, with the additional property that one cannot "overflow...

23/5,K/5 (Item 4 from file: 349)
DIALOG(R)File 349:PCT FULLTEXT

00475798 **Image available**
ENCRYPTION DEVICES FOR USE IN A CONDITIONAL ACCESS SYSTEM
DISPOSITIFS DE CRYPTAGE POUR SYSTEME A ACCES CONDITIONNEL
Patent Applicant/Assignee:
SCIENTIFIC-ATLANTA INC,
Inventor(s):
PALGON Michael S,
PINDER Howard G,
Patent and Priority Information (Country, Number, Date):
Patent: WO 9907150 A1 19990211
Application: WO 98US16145 19980731 (PCT/WO US9816145)
Priority Application: US 9754575 19970801
Designated States: AL AM AT AU AZ BA BB BG BR BY CA CH CN CU CZ DE DK EE ES FI GB GE GH GM HR HU ID IL IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MD MG MK MN MW MX NO NZ PL PT RO RU SD SE SG SI SK SL TJ TM TR TT UA UG UZ VN YU ZW GH GM KE LS MW SD SZ UG ZW AM AZ BY KG KZ MD RU TJ TM AT BE CH CY DE DK ES FI FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN GW ML MR NE SN TD TG
Main International Patent Class: **H04N-007/16**
International Patent Class: **H04N-007/167**
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 33492

English Abstract
A cable television system provides conditional access to services. The cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

French Abstract
La presente invention concerne un reseau de televiseur par cable fournissant un acces conditionnel a des services et comprenant une tete de bus depuis laquelle sont diffuses les "instances" de services, ou programmes, ainsi qu'une pluralite de coffrets d'abonnes permettant aux abonnes de recevoir et de decrypter selectivement les instances pour les

regarder. Les instances de services sont cryptees en utilisant des clefs publiques et/ou privees fournies par des fournisseurs de services ou des centraux d'autorisation. Les clefs qu'utilisent les coffrets d'abonnes pour le decryptage selectionne peuvent etre a caractere privees ou publiques, et reaffectees a differents moments pour offrir un reseau de television par cable peu sensible aux piratages.

Main International Patent Class: **H04N-007/16**
International Patent Class: **H04N-007/167**
Fulltext Availability:
Claims

Claim
... ftu-ther comprising:
the entitlement agent coupled to the controller for generating an instance of service;
a **random number generator** for generating a multi-session **key** (MSK);
a **processor** coupled to the **random number generator** and the controller for hashing the instance of service and the MSK in a secure one-way hash to **generate** a digest that is included as a part of the information.
88
SUBSTITUTE SHEET (RULE 26)
. The...

...36, further comprising:
an encryptor coupled to the controller for further encrypting the information using a public **key** associated with the service reception component prior to transmission of the information.

38 The service origination component...terminal.

47 The cable television system of claim 4'),, wherein the service origination component further comprises:
a **random number generator** for generating a multi-session **key** (MSK);
a **processor** coupled to the **random number generator** and the controller for hashing an instance of service and the MSK in a secure one-way hash to **generate** a digest that is included as a part of the information.
90
SUBSTITUTE SHEET (RULE 26)
. The...

...message including the digest, wherein the entitlement management message is encrypted by the processor using the private **key** to **generate** the information that is transmitted to the service reception component.

49 The cable television system of claim...

23/5,K/6 **(Item 5 from file: 349)**
DIALOG(R)File 349:PCT FULLTEXT

00268269
ENHANCING OPERATIONS OF VIDEO TAPE CASSETTE PLAYERS
PERFECTIONNEMENT DU FONCTIONNEMENT DE LECTEURS DE CASSETTE VIDEO
Patent Applicant/Assignee:
YUEN Henry C,
KWOH Daniel S,
MANKOVITZ Roy J,
HINDMAN Carl,
NGAI Hing Y,

Inventor(s):
YUEN Henry C,
KWOH Daniel S,
MANKOVITZ Roy J,
HINDMAN Carl,
NGAI Hing Y,

Patent and Priority Information (Country, Number, Date):
Patent: WO 9416441 A1 19940721
Application: WO 94US173 19940105 (PCT/WO US9400173)
Priority Application: US 931125 19930105; US 9314541 19930208
Designated States: AT AU BB BG BR BY CA CH CN CZ DE DK ES FI GB HU JP KP KR KZ LK LU MG MN MW NL NO NZ PL PT RO RU SD SE SK UA US VN AT BE CH DE DK ES FR GB GR IE IT LU MC NL PT SE BF BJ CF CG CI CM GA GN ML MR NE SN TD TG
Main International Patent Class: **G11B-015/18**
International Patent Class: **G11B-15:22** ; **H04N-07:08** ; **H04N-07:087** ; **H04N-07:167** ; **H04N-07:173** ; **H04N-05:78** ; **H04N-05:50** ; G04G-07:00
Publication Language: English
Fulltext Availability:
Detailed Description
Claims
Fulltext Word Count: 76305

English Abstract
Operation of a video cassette player (10) is facilitated by providing a vertical blanking interval decoder (60a) which decodes information such as title, date, time and length of broadcast programs and utilizing the information in providing a directory of the programs (33a) as well as control of the VCR. The VCR is also provided with a VBI encoder (60b) for inserting control as well as directory information into the tape, either in portions of the video track (13) or in the control track (11).

French Abstract
Le fonctionnement d'un lecteur de cassettes video (10) est facilite par la mise en place d'un decodeur d'intervalle de suppression de trame (60a) qui decode des informations telles que le titre, la date, l'heure et la duree des programmes de radiodiffusion. Ces informations sont utilisees pour creer un repertoire des programmes (33a) ainsi que pour la commande du magnetoscope. Ce dernier est egalement equipe d'un codeur d'intervalle de suppression de trame (60b) permettant d'inserer sur la bande des informations relatives a la commande ainsi qu'au repertoire, soit dans des parties de la piste video (13), soit dans la piste de commande (11).

Main International Patent Class: **G11B-015/18**
International Patent Class: **G11B-15:22** ...

... **H04N-07:08** ...

... **H04N-07:087** ...

... **H04N-07:167** ...

... **H04N-07:173** ...

... **H04N-05:78** ...
... **H04N-05:50**
Fulltext Availability:
Detailed Description

Detailed Description
... address marks are written at I minute intervals onto the control track of a VHS tape. In **computer** backup of hard discs by tape, the streaming mode is usually used where a constant stream of...beginning of each program on the tape and at the end of the tape.

The TID is **generated** by seeding a **random number generator** with the time of the first usage of the VCR so that the probability of two

```
Set     Items   Descriptio
S1       2531   RANDOM (N) (SEQUENC? OR NUMBER? OR NUMERIC?)()GENERATOR?
S2    6407358   GENERATE? OR REPRODUCE? OR CREATE? OR PRODUCE? OR DEVELOP?
S3      12812   NONCE OR RANDOM()(SEQUENCE? OR NUMBER? OR NUMERIC)
S4     688084   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE OR ENCIP-
            HER? OR CODING OR CODED OR ENCOD?
S5     650356   BUS OR BUSES OR PATHWAY OR CHANNEL
S6       6361   (SECRET OR PRIVATE OR CRYPTO?)()(KEY OR KEYS OR CODE?) OR -
            PKI
S7         25   (PORTION OR PART OR SECTION)(3N)((DATA OR INFORMATION OR F-
            ACT?)()(SEGMENT? OR PIECE? OR BLOCK? OR CHUNK? OR BITS OR BYT-
            ES))
S8    2198619   DISTRIBUTION OR ALLOCATION OR DISSEMINATION OR DISPERSAL OR
             DISPERSION OR DISTRIBUTE?
S9       5740   (DEVICE? OR CLIENT? OR PC OR COMPUTER? OR WORKSTATION? OR -
            WORK()STATION? OR NODE? OR TERMINAL? OR PROCESSOR)(2N)(KEY OR
            KEYS)
S10      1037   S1 AND S2 AND S3
S11       315   S5 AND S6
S12         0   S7 AND ((KEY OR KEYS)(3N) S8)
S13         1   S7 AND (KEY OR KEYS)
S14         0   S10 AND S11 AND S9
S15         0   S10 AND S11
S16         7   S10 AND S9
S17         7   S10 AND S9
S18         0   S7 AND S8 AND S9
S19         0   S7 AND S8 AND (KEY OR KEYS)
S20         8   S13 OR S16 OR S17
S21         5   S20 NOT PY>2001
S22         5   S21 NOT PD>20010329
File   8:Ei Compendex(R) 1970-2004/Mar W3
         (c) 2004 Elsevier Eng.  Info. Inc.
File  35:Dissertation Abs Online 1861-2004/Mar
         (c) 2004 ProQuest Info&Learning
File 202:Info. Sci. & Tech. Abs. 1966-2004/Feb 27
         (c) 2004 EBSCO Publishing
File  65:Inside Conferences 1993-2004/Mar W4
         (c) 2004 BLDSC all rts. reserv.
File   2:INSPEC 1969-2004/Mar W3
         (c) 2004 Institution of Electrical Engineers
File 233:Internet & Personal Comp. Abs. 1981-2003/Sep
         (c) 2003 EBSCO Pub.
File  94:JICST-EPlus 1985-2004/Mar W2
         (c)2004 Japan Science and Tech Corp(JST)
File  99:Wilson Appl. Sci & Tech Abs 1983-2004/Feb
         (c) 2004 The HW Wilson Co.
File  95:TEME-Technology & Management 1989-2004/Mar W2
         (c) 2004 FIZ TECHNIK
File 583:Gale Group Globalbase(TM) 1986-2002/Dec 13
         (c) 2002 The Gale Group
```

22/5/1 (Item 1 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

06336666 E.I. No: EIP03137413838
Title: Elliptic curve random number **generation**
Author: Lee, Lap-Piu; Wong, Kwok-Wo
Corporate Source: Department of Electronic Engineering City University of Hong Kong, Kowloon Tong, Hong Kong
Conference Title: IEEE Region 10 International Conference on Electrical and Electronic Technology
Conference Location: Singapore, Singapore Conference Date: 20010819-20010822
Sponsor: IEEE Region 10
E.I. Conference No.: 60749
Source: IEEE Region 10 International Conference on Electrical and Electronic Technology 2001. (IEEE cat n 01CH37239)
Publication Year: 2001
ISBN: 0780371011
Language: English
Document Type: CA; (Conference Article) Treatment: T; (Theoretical)
Journal Announcement: 0303W5
Abstract: A **random number generator** based on the addition of the points on an elliptic curve over finite fields is proposed. By using the proposed generator with Elliptic Curve Cryptographic (ECC) system together, we can save hardware and software components. Since the proposed **random number generator** is based on the core operation of ECC, it can be designed and implemented efficiently using the existing components. The period of the bit sequences is analyzed theoretically. Moreover, Sequences **produced** by this generator have passed the FIPS 140-2 statistical tests of the Cryptographic Standards and Validation Programs at NIST. As a result, the proposed generator is found suitable to be a **random number generator** . 11 Refs.
Descriptors: **Random number** generation; Public **key** cryptography; **Computer** hardware; Computer software; Polynomials
Identifiers: Elliptic curves; Finite fields
Classification Codes:
922.2 (Mathematical Statistics); 921.1 (Algebra)
922 (Statistical Methods); 723 (Computer Software, Data Handling & Applications); 722 (Computer Hardware); 921 (Applied Mathematics)
92 (ENGINEERING MATHEMATICS); 72 (COMPUTERS & DATA PROCESSING)

22/5/2 (Item 2 from file: 8)
DIALOG(R)File 8:Ei Compendex(R)

05938590 E.I. No: EIP01466730170
Title: Building the IBM 4758 secure coprocessor
Author: Dyer, J.G.; Lindemann, M.; Perez, R.; Sailer, R.; Van Doorn, L.; Smith, S.W.; Weingart, S.
Corporate Source: IBM T.J. Watson Research Center, Hawthorne, NY, United States
Source: Computer v 34 n 10 October 2001. p 57-66
Publication Year: 2001
CODEN: CPTRB4 ISSN: 0018-9162
Language: English
Document Type: JA; (Journal Article) Treatment: G; (General Review)
Journal Announcement: 0111W3
Abstract: IBM's Common Cryptoraphic Architecture product group realized that its next-generation product required properties possessed by the secure coprocessor that IBM Research advocated. This knowledge gave the research team a unique and perhaps nonrepeatable opportunity. Meeting the challenge of building a user-configurable secure coprocessor provided several lessons in hardware and software **development** and continues to spur further research. (Edited abstract) 10 Refs.
Descriptors: Security of data; Program processors; Computer hardware;

Software engineering; Computer crime; Public **key** cryptography; Interfaces (**computer**); Firmware; Network protocols; ROM; Random access storage; Encoding (symbols); Computer operating systems
Identifiers: Coprocessor; Public key interfaces; Common cryptographic architecture; Hardware tamper response; **Random number generators** ; Authentication; Application programming interface
Classification Codes:
723.2 (Data Processing); 723.1 (Computer Programming); 722.2 (Computer Peripheral Equipment); 722.1 (Data Storage, Equipment & Techniques)
723 (Computer Software, Data Handling & Applications); 722 (Computer Hardware)
72 (COMPUTERS & DATA PROCESSING)

22/5/3 (Item 1 from file: 2)
DIALOG(R)File 2:INSPEC

02645502 INSPEC Abstract Number: C86025507
Title: A current view of random number generators
Author(s): Marsaglia, G.
Author Affiliation: Dept. of Comput. Sci., Washington State Univ., Pullman, WA, USA
Conference Title: Computer Science and Statistics. Proceedings of the Sixteenth Symposium on the Interface p.3-10
Editor(s): Billard, L.
Publisher: North-Holland, Amsterdam, Netherlands
Publication Date: 1985 Country of Publication: Netherlands xi+296 pp.
ISBN: 0 444 87725 8
Conference Date: March 1984 Conference Location: Atlanta, GA, USA
Language: English Document Type: Conference Paper (PA)
Treatment: Theoretical (T); Experimental (X)
Abstract: The ability to **generate** satisfactory sequences of **random numbers** is one of the **key** links between **Computer** Science and Statistics. Standard methods may no longer be suitable for increasingly sophisticated uses, such as in precision Monte Carlo studies, testing for primes, combinatorics, or public encryption schemes. This article describes stringent new tests for which standard **random number generators** : congruential, shift-register and lagged-Fibonacci, give poor results, and describes new methods that pass the stringent tests and seem more suitable for precision Monte Carlo use. (14 Refs)
Subfile: C
Descriptors: **random number** generation; statistics
Identifiers: combining simple generators; randomness testing; **random number generators** ; Monte Carlo studies; congruential; shift-register; lagged-Fibonacci
Class Codes: C1140Z (Other and miscellaneous); C7310 (Mathematics); C7400 (Engineering)

22/5/4 (Item 2 from file: 2)
DIALOG(R)File 2:INSPEC

00446972 INSPEC Abstract Number: C72023920
Title: Information retrieval system
Assignee(s): Western Electric Co. Inc
Patent Number: GB 1279459 Issue Date: 720628
Application Date: 690716
Priority Appl. Number: US 745738 Priority Appl. Date: 680718
Country of Publication: UK
Language: English Document Type: Patent (PT)
Treatment: Practical (P)
Abstract: The system referred to consists of a magnetic memory divided into parts each of which stores data blocks and **key** words corresponding to blocks stored in another part of the memory, the data blocks are accessed from the memory parts in sequence and successive **key** words are

compared with associati[redacted] data block requests to ena[redacted] the accessing system to retrieve a desired block. Preferably each data block has a unique address in its memory **part** , and a matching **data block** address is stored in a register forming part of the accessing system.

Subfile: C

Descriptors: information retrieval systems; magnetic storage systems; storage management

Identifiers: information retrieval system; magnetic memory; address; accessing system

Class Codes: C5320E (Storage on stationary magnetic media); C7250 (Information storage and retrieval)

22/5/5 (Item 1 from file: 95)

00555596 E92043544089

Analysis of pseudo random sequences generated **by cellular automata**
(Analyse von durch zellulaere Automaten erzeugte Pseudozufallsfolgen)

Meier, W; Staffelbach, O
HTL Brugg-Windisch, CH; GRETAG Regensdorf, CH

EUROCRYPT '91, Advances in Cryptology, Workshop on the Theory and Application of Cryptographic Techniques, Brighton, GB, April 8-11, 19911991
Document type: Conference paper Language: English
Record type: Abstract
ISBN: 3-540-54620-0; 0-387-54620-0

ABSTRACT:
The security of cellular automata for stream cipher applications is investigated. A cryptanalytic algorithm is **developed** for a known plaintext attack where the plaintext is assumed to be known up to the unicity distance. The algorithm is shown to be successful on small **computers** for **key** sizes up to N between 300 and 500 bits. For a cellular automation to be secure against more powerful adversaries it is concluded that the key size N needs to be about 1000 bits. The cryptanalytic algorithm takes advantage of an equivalent description of the cryptosystem in which the keys are not equiprobable. It is shown that key search can be reduced considerably if one is contented to succeed only with a certain success probability. This is established by an information theoretic analysis of arbitrary key sources with non-uniform probability distribution.

DESCRIPTORS: AUTOMATON; MULTIPROCESSING SYSTEMS; **RANDOM SEQUENCE** ; CIPHERING--ENCRYPTION; **RANDOM NUMBER GENERATORS** ; DATA INTEGRITY
IDENTIFIERS: ZELLULAERER AUTOMAT; CHIFFRETEXT; RUECKKOPPLUNGSREGISTER; KLARTEXT; SCHLUESSELSYSTEM; Verschluesselung; zellulaerer Automat

```
Set     Items   Description
S1       3349   RANDOM (N) (SEQUENC? OR NUMBER? OR NUMERIC?)()GENERATOR?
S2    3465673   GENERATE? OR REPRODUCE? OR CREATE? OR PRODUCE? OR DEVELOP?
S3      12261   NONCE OR RANDOM()(SEQUENCE? OR NUMBER? OR NUMERIC)
S4     492945   ENCRYPT? OR SCRAMBL? OR CIPHER? OR CRYPT? OR CODE OR ENCIP-
            HER? OR CODING OR CODED OR ENCOD?
S5     622809   BUS OR BUSES OR PATHWAY OR CHANNEL
S6       5419   (SECRET OR PRIVATE OR CRYPTO?)()(KEY OR KEYS OR CODE?) OR -
            PKI
S7       7281   (PORTION OR PART OR SECTION)(3N)((DATA OR INFORMATION OR F-
            ACT?)()(SEGMENT? OR PIECE? OR PART? OR BLOCK? OR CHUNK? OR BI-
            TS OR BYTES))
S8     759944   DISTRIBUTION OR ALLOCATION OR DISSEMINATION OR DISPERSAL OR
             DISPERSION OR DISTRIBUTE?
S9      12634   (DEVICE? OR CLIENT? OR PC OR COMPUTER? OR WORKSTATION? OR -
            WORK()STATION? OR NODE? OR TERMINAL? OR PROCESSOR)(2N)(KEY OR
            KEYS)
S10      1837   S1 AND S2 AND S3
S11       242   S5 AND S6
S12         7   S7 AND ((KEY OR KEYS)(3N)S8)
S13         0   S10 AND S11 AND S12 AND S9
S14        31   S10 AND S9
S15         1   S14 AND S11
S16       272   S10 AND (KEY OR KEYS)
S17         0   S10 AND S11 AND S12 AND S14 AND S16
S18         4   S10 AND S11
S19        31   S10 AND S14
S20         4   S11 AND S16
S21        31   S16 AND S19
S22        41   S12 OR S14 OR S15 OR S19 OR S20
S23         7   S22 AND IC=(G11B? OR H04N?)
S24       205   S4 (3N) S5 (3N) (KEY OR KEYS)
S25     25829   (DATA OR INFORMATION OR FACT?)()S5
S26         3   S24 AND S25 AND S9
S27         2   S7 AND S8 AND S9
S28        21   S7 AND S8 AND (KEY OR KEYS)
S29        24   S26 OR S27 OR S28
S30         7   S29 AND IC=(G11B? OR H04N?)
S31        12   S23 OR S30
File 347:JAPIO Nov 1976-2003/Nov(Updated 040308)
         (c) 2004 JPO & JAPIO
File 350:Derwent WPIX 1963-2004/UD,UM &UP=200417
         (c) 2004  Thomson Derwent
```

31/5/1 (Item 1 from file: 347)
DIALOG(R)File 347:JAPIO

07475922 **Image available**
DATA-REPRODUCING DEVICE AND DATA REPRODUCING METHOD, DATA REPRODUCING PROGRAM AND VIDEO-ON-DEMAND SYSTEM

PUB. NO.: 2002-344440 [JP 2002344440 A]
PUBLISHED: November 29, 2002 (20021129)
INVENTOR(s): OGAMI AKIHIRO
APPLICANT(s): TOSHIBA CORP
APPL. NO.: 2001-150968 [JP 2001150968]
FILED: May 21, 2001 (20010521)
INTL CLASS: H04L-009/08; **G11B-020/10** ; H04L-009/16; **H04N-005/93** ; **H04N-007/173**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a data reproducing device, capable of instantaneously starting the reproduction of digital data by shortening an access time, since the reproduction of digital data is instructed by a user, until the reproduction of digital data is actually started.

SOLUTION: The preceding **data part** of digital data obtained, by converting information such as characters, voices, static images, and moving images into digital signals is non-enciphered, and only the subsequent **data part** is enciphered, and the digital data are **distributed** to a client. When the reproduction of the digital data is instructed, a **client** requests **key** data for solving the cryptograph to a server and reproduces the leading **data part** of the digital data in parallel.

31/5/2 (Item 2 from file: 347)
DIALOG(R)File 347:JAPIO

07129863 **Image available**
OPTICAL DISK, ITS RECORDER, RECORDING METHOD AND REPRODUCING DEVICE

PUB. NO.: 2001-357533 [JP 2001357533 A]
PUBLISHED: December 26, 2001 (20011226)
INVENTOR(s): MIYASHITA SEIJUN
ISHIBASHI HIROMICHI
TANAKA SHINICHI
YUMIBA TAKASHI
APPLICANT(s): MATSUSHITA ELECTRIC IND CO LTD
APPL. NO.: 2000-185374 [JP 2000185374]
FILED: June 20, 2000 (20000620)
PRIORITY: 11-192760 [JP 99192760], JP (Japan), July 07, 1999 (19990707)
11-201382 [JP 99201382], JP (Japan), July 15, 1999 (19990715)
2000-109602 [JP 2000109602], JP (Japan), April 11, 2000 (20000411)
INTL CLASS: **G11B-007/007** ; **G11B-007/24** ; **G11B-019/02** ; **G11B-019/04** ; **G11B-020/10**

ABSTRACT

PROBLEM TO BE SOLVED: To provide an optical disk recorder or the like which is capable of preventing the illicit copying of the whole of an optical disk recorded with digital written works as it is.

SOLUTION: This optical disk device has a formatter 1 which forms the **channel** signal corresponding to main digital information, a **secret key** memory section 1c which stores sub-digital information (**secret key**), a pseudo **random - number generator** 2 which **generates** pseudo **random -**

number sequences, an [redacted]R 4 which logically inverts the [redacted]seudo- **random** **number** sequences in accordance with the respective bits of the **secret** **key** , a PE modulator 5 which forms a PE modulation signal in accordance with the logically inverted pseudo **random** - **number** sequences, a phase modulator 6 which advances the phase of the edge of the **channel** signal by a specified slight time when the PE modulation signal is '1' and delays the phase of the edge of the **channel** signal by a specified slight time when the PE modulation signal is '0' and a recording **channel** 7 for forming recording marks in a DVD 9 based on the **channel** signal to be modulated which is formed by the phase modulator 6.

31/5/3 (Item 3 from file: 347)
DIALOG(R)File 347:JAPIO

06950264 **Image available**
DATA OPERATION METHOD, RECORDING MEDIUM FOR RECORDING PROGRAM OF IMAGE GENERATING METHOD, TRANSMISSION MEDIUM FOR TRANSMITTING THE PROGRAM OF THE IMAGE GENERATING METHOD, RECORDING MEDIUM FOR RECORDING PROGRAM OF IMAGE DECODING METHOD AND TRANSMISSION MEDIUM FOR TRANSMITTING THE PROGRAM OF THE IMAGE DECODING METHOD

PUB. NO.: 2001-177816 [JP 2001177816 A]
PUBLISHED: June 29, 2001 (20010629)
INVENTOR(s): HIRANO HIDEYUKI
KOTANI MASATAKE
HASHIMOTO SHINJI
MURAMOTO KAZUHIKO
APPLICANT(s): FUJITSU LTD
APPL. NO.: 11-357131 [JP 99357131]
FILED: December 16, 1999 (19991216)
INTL CLASS: **H04N-007/167** ; G06F-012/14; G06F-015/00; G06F-017/60; G06T-001/00; **H04N-001/387** ; **H04N-007/08** ; **H04N-007/081**

ABSTRACT

PROBLEM TO BE SOLVED: To provide a data operation method that facilitates the utilization by legal users without losing the author's copyright and the copyright of digital contents.

SOLUTION: Part of digital contents 11 is copied to generate a partial **data** **part** 43, which is encrypted by using a contents **key** 45, the contents **key** 45 and image composite information 42 are encrypted by an encryption **key** 47 to generate permission information 48, contents information 41 is visibly embedded to the digital contents 11, a **data** **part** 50 with the permission information to which the permission information 48 is embedded as invisible information and an encrypted partial **data** **part** 46 are composited to generate composite data 60, which are **distributed** .

31/5/4 (Item 4 from file: 347)
DIALOG(R)File 347:JAPIO

06514352 **Image available**
COPY PROTECTING METHOD, DATA PROCESSOR APPLYING THE METHOD AND RECORDING MEDIUM

PUB. NO.: 2000-100069 [JP 2000100069 A]
PUBLISHED: April 07, 2000 (20000407)
INVENTOR(s): ISHIBASHI YASUHIRO
HARUKI KOUSUKE
KATO HIROSHI

APPLICANT(s): TOSHIBA CORP
APPL. NO.: 10-267505 [JP 98267505]
FILED: September 22, 1998 (19980922)
INTL CLASS: **G11B-020/10** ; G09C-001/00; H04L-009/32; **H04N-007/16**

ABSTRACT

PROBLEM TO BE SOLVED: To use similarly enciphered contents data among respective equipments in common and to realize a firm copy protecting method.

SOLUTION: A seed key (Kcs) **generated** by a **random number generator** , etc., is **produced** by a source device, and the seed key (Kcs) is subjected to encipherment by utilizing a combination key (Kck), and the enciphered seed key (eKcs) is transmitted to a sink device. By the source **device** , a contents **key** (Kc) for ciphering and deciphering contents data (Contents) is **produced** .in accordance with the function between the seed key (Kcs). and independent variable data (Nc). Thus, the enciphered contents data (e [Contents (KC)]) are deciphered by using the contents key (Kc).

31/5/5 (Item 5 from file: 347)
DIALOG(R)File 347:JAPIO

05207619 **Image available**
SCRAMBLE OR DESCRAMBLE METHOD AND SCRAMBLE OR DESCRAMBLE DEVICE FOR PACKET SIGNAL

PUB. NO.: 08-163119 [JP 8163119 A]
PUBLISHED: June 21, 1996 (19960621)
INVENTOR(s): KIMURA TAKESHI
NANBA SEIICHI
APPLICANT(s): NIPPON HOSO KYOKAI <NHK> [000435] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 06-304854 [JP 94304854]
FILED: December 08, 1994 (19941208)
INTL CLASS: [6] H04L-009/06; H04L-009/14; G09C-001/10; **H04N-007/167**
JAPIO CLASS: 44.3 (COMMUNICATION -- Telegraphy); 34.4 (SPACE DEVELOPMENT -- Communication); 44.6 (COMMUNICATION -- Television); 44.9 (COMMUNICATION -- Other)

ABSTRACT

PURPOSE: To easily cope with various contract/charging forms by allocating one of plural scramble **key** candidates to the **distribution** of scramble **keys** and also allocating other **key** candidates to the program element groups respectively.

CONSTITUTION: A scramble **key** selector means 3 selects one of **key** candidates 31, 32 and 33 which are read out of the **key** candidate storage areas 21, 22 and 23 of a scramble **key** storage means 2 based on the scramble **key** selection information on the header part of an unprocessed packet signal 5. Then the means 3 sends the selected **key** candidate to a scramble/descramble means 4 as a scramble **key** 7. The **key** 7 scrambles and descrambles the **data** . **part** of the signal 5 and outputs a processed packet signal 6. The selection of the 1st **key** candidates 11 and 31 are limited in a time band when the scramble **keys** can be **distributed** and therefore (N-1) pieces of **key** candidates are available when the total number of **key** candidates is equal to N. These **key** candidates are allocated to M types of program element groups respectively and the scramble/descramble operations are carried out. When M program element groups are more than (N-1) **key** candidates, the M groups are duplicated.

31/5/6 (Item 6 from file: 347)
DIALOG(R)File 347:JAPIO

04506548 **Image available**
DIGITAL SIGNAL REPRODUCING DEVICE

PUB. NO.: 06-150448 [JP 6150448 A]
PUBLISHED: May 31, 1994 (19940531)
INVENTOR(s): ASANO TAKASHI
APPLICANT(s): SONY CORP [000218] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 04-294651 [JP 92294651]
FILED: November 02, 1992 (19921102)
INTL CLASS: [5] **G11B-015/087** ; **G11B-015/087** ; **G11B-020/10** ; **G11B-020/10** ; **G11B-027/28**
JAPIO CLASS: 42.5 (ELECTRONICS -- Equipment)
JAPIO KEYWORD: R131 (INFORMATION PROCESSING -- Microcomputers & Microprocessers)
JOURNAL: Section: P, Section No. 1795, Vol. 18, No. 473, Pg. 33, September 02, 1994 (19940902)

ABSTRACT

PURPOSE: To improve a handleability by retrieving a sampling frequency **distribution** and a retrieval **key** in combination.

CONSTITUTION: A **key** changing over to a display of sampling frequency **distribution** , a scanning **key** reproducing a specified time signal after performing a music program searching, and a program searching **key** performing the music program searching, are provided in the signal reproducing device. When a display device of the reproducing device is changed over to the display of sampling frequency **distribution** and also the scanning **key** is pushed, an operation input signal from the **key** switch 2 is transmitted to a main CPU 4 through a display processing circuit 3. By the CPU 4, the sampling frequency of a subcode part in the region of a main **data part** is retrieved and the changed point of sampling frequency existing in the part backward from the present reproducing position is retrieved, then the specified time recording signal is reproduced while making the detected time point to the reproduction start position. In the case the program searching **key** is pushed, the changed point of the sampling frequency existing in the part forward or backward from the present reproducing position by the number of **key** pushing times is detected, thereby the program searching is performed.

31/5/7 (Item 7 from file: 347)
DIALOG(R)File 347:JAPIO

03677361 **Image available**
MAGNETIC DISK CONTROLLER

PUB. NO.: 04-042461 [JP 4042461 A]
PUBLISHED: February 13, 1992 (19920213)
INVENTOR(s): OKA YOSHIJI
APPLICANT(s): NEC CORP [000423] (A Japanese Company or Corporation), JP (Japan)
APPL. NO.: 02-151064 [JP 90151064]
FILED: June 08, 1990 (19900608)
INTL CLASS: [5] **G11B-019/02** ; G06F-003/06
JAPIO CLASS: 42.5 (ELECTRONICS -- Equipment); 45.3 (INFORMATION PROCESSING -- Input Output Units)
JAPIO KEYWORD: R131 (INFORMATION PROCESSING -- Microcomputers & Microprocessers)
JOURNAL: Section: P, Section No. 1358, Vol. 16, No. 220, Pg. 46, May 22, 1992 (19920522)

ABSTRACT

PURPOSE: To prevent malfunction when accessing an allocated record

occurring by storing the number of records allocatable one track and that of records when reading one track after **allocation** , and comparing those numbers of records.

CONSTITUTION: This controller is comprised of a bus controller 5, a processor 6, a first logic circuit 8 which calculates and stores the length of a **key part** and a **data part** sent from software and the number of records allocatable to one track from the number of data transfer, a second logic circuit 9 which stores the number of records when one track is read after the **allocation** , and a comparator 7 which compares the numbers of records stored in the logic circuits 8 and 9. The comparator 7 sends a comparison result to the processor 6, and the processor 6 reports normal completion when coincidence is obtained between them and abnormal completion when noncoincidence is obtained to a central processing unit via a communication bus 2. Thereby, it is possible to prevent the malfunction occurring when accessing the record allocated next.

31/5/8 (Item 1 from file: 350)
DIALOG(R)File 350:Derwent WPIX

015006683 **Image available**
WPI Acc No: 2003-067200/200306
Related WPI Acc No: 2003-110651
XRPX Acc No: N03-052179

Copy protection system for DVD, CD-ROM, encrypts **disk data using** encryption bus key **derived based on** key **distribution data block,** device keys **and random number**

Patent Assignee: INTEL CORP (ITLC); RIPLEY M S (RIPL-I); TRAW B S (TRAW-I)
Inventor: RIPLEY M; TRAW B; RIPLEY M S; TRAW B S

Number of Countries: 101 Number of Patents: 003
Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week
US 20020141577	A1	20021003	US 2001823423	A	20010329	200306 B
WO 200280170	A2	20021010	WO 2002US7085	A	20020307	200306
EP 1374237	A2	20040102	EP 2002721303	A	20020307	200409
			WO 2002US7085	A	20020307	

Priority Applications (No Type Date): US 2001823423 A 20010329
Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
US 20020141577	A1		11	H04N-007/167	
WO 200280170	A2	E		G11B-020/00	

Designated States (National): AE AG AL AM AT AU AZ BA BB BG BR BY BZ CA CH CN CO CR CU CZ DE DK DM DZ EC EE ES FI GB GD GE GH GM HR HU ID IL IN IS JP KE KG KP KR KZ LC LK LR LS LT LU LV MA MD MG MK MN MW MX MZ NO NZ OM PH PL PT RO RU SD SE SG SI SK SL TJ TM TN TR TT TZ UA UG UZ VN YU ZA ZM ZW
Designated States (Regional): AT BE CH CY DE DK EA ES FI FR GB GH GM GR IE IT KE LS LU MC MW MZ NL OA PT SD SE SL SZ TR TZ UG ZM ZW

EP 1374237 A2 E G11B-020/00 Based on patent WO 200280170
Designated States (Regional): AL AT BE CH CY DE DK ES FI FR GB GR IE IT LI LT LU LV MC MK NL PT RO SE SI TR

Abstract (Basic): US 20020141577 A1

NOVELTY - An encryption subsystem encrypts data accessed from a disk using an **encryption key** prior to transmitting the **encrypted** data through a **data bus** . The **encryption key** is derived based on a **key** distribution data block, **device keys** assigned to the encryption subsystem and a random number.

DETAILED DESCRIPTION - INDEPENDENT CLAIMS are included for the following:

(1) Copy protection method; and
(2) Copy protection apparatus.

USE - For protecting digital content stored on a storage medium

such as DVD, CD-ROM, optical disk, magneto-optical disk, flash-based memory, floppy disk, hard drive, ROM, RAM, EPROM, EEPROM, magnetic or optical cards, from unauthorized copying.

ADVANTAGE - Effectively improves the protection of digital content transmitted over bus and protects the content against reply attack by using the random number to generate the encryption key.

DESCRIPTION OF DRAWING(S) - The figure shows a flowchart illustrating DVD contents decrypting and descrambling procedure.

pp; 11 DwgNo 5/5

Title Terms: COPY; PROTECT; SYSTEM; CD; ROM; DISC; DATA; ENCRYPTION; BUS; KEY; DERIVATIVE; BASED; KEY; DISTRIBUTE; DATA; BLOCK; DEVICE; KEY; RANDOM ; NUMBER

Derwent Class: T01; T03

International Patent Class (Main): **G11B-020/00 ; H04N-007/167**

File Segment: EPI

31/5/9 (Item 2 from file: 350)

DIALOG(R)File 350:Derwent WPIX

011449712 **Image available**

WPI Acc No: 1997-427619/199740

XRPX Acc No: N97-355925

Key distribution system for secure communication - uses random number generator **in terminal to prepare encryption or decryption keys according to** random numbers generated **by communication apparatus and** terminal , **and secret** key **held by both**

Patent Assignee: OKI ELECTRIC IND CO LTD (OKID); CASIO COMPUTER CO LTD (CASK); OKI DENKI KOGYO KK (OKID)

Inventor: KAWANO K; KIZAKI M; SHONA Y

Number of Countries: 008 Number of Patents: 006

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
EP 793367	A2	19970903	EP 97102667	A	19970219	199740	B
JP 9238132	A	19970909	JP 9643315	A	19960229	199746	
KR 97063006	A	19970912	KR 976751	A	19970228	199840	
TW 335581	A	19980701	TW 97102459	A	19970227	199846	
CN 1211776	A	19990324	CN 97104897	A	19970228	199931	
US 6018581	A	20000125	US 97808542	A	19970228	200012	

Priority Applications (No Type Date): JP 9643315 A 19960229

Cited Patents: No-SR.Pub

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
EP 793367	A2	E	15	H04L-009/08	
Designated States (Regional): DE FR GB					
JP 9238132	A		10	H04L-009/08	
US 6018581	A			H04L-009/00	
KR 97063006	A			G09C-005/00	
TW 335581	A			H04L-009/32	
CN 1211776	A			G09C-005/00	

Abstract (Basic): EP 793367 A

The communication system includes a communication apparatus for reception or transmission and a terminal provided with a memory in which data for specifying function of the communication apparatus are stored. The communication apparatus and the terminal each include a **random number** generating unit for generating a **random number** . An encryption/decryption key preparing unit is used for preparing an encryption/decryption key on the basis of both **random numbers generated** by the respective **random number** generating units of the communication apparatus and the terminal and a secret key held in common by both.

An encryption/decryption processing unit encrypts or decrypts communication data between the communication apparatus and the terminal. It includes the data by using the encryption/decryption key.

USE/ADVANTAGE - Maintains higher security even if communication is monitored. Makes alteration or forgery difficult.

Dwg.1/6

Title Terms: KEY; DISTRIBUTE; SYSTEM; SECURE; COMMUNICATE; RANDOM; NUMBER; GENERATOR; TERMINAL; PREPARATION; ENCRYPTION; DECRYPTER; KEY; ACCORD; RANDOM; NUMBER; **GENERATE** ; COMMUNICATE; APPARATUS; TERMINAL; SECRET; KEY ; HELD

Derwent Class: P85; W01

International Patent Class (Main): G09C-005/00; H04L-009/00; H04L-009/08; H04L-009/32

International Patent Class (Additional): G06K-017/00; G09C-001/00; **H04N-007/16**

File Segment: EPI; EngPI

31/5/10 (Item 3 from file: 350)

DIALOG(R)File 350:Derwent WPIX

010760537 **Image available**

WPI Acc No: 1996-257492/199626

XRPX Acc No: N96-216641

Facsimile - has code key varying part that changes secret code key used in code communication according to random number generated **by** random number generator

Patent Assignee: MITA IND CO LTD (MTAI)

Number of Countries: 001 Number of Patents: 001

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 8107411	A	19960423	JP 94239856	A	19941004	199626	B

Priority Applications (No Type Date): JP 94239856 A 19941004

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 8107411	A		12	H04L-009/00	

Abstract (Basic): JP 8107411 A

The device performs a code communication by using a secret code **key** The **device** enciphers a communication information in which transmitting and receiving is possible. A **random - number** generating unit outputs **random numbers** according to a predetermined rule.

A code key varying part changes the secret code key according to the output of the **random - number** generating unit. A transmitter sends a routine information which includes the transmit value of the **random number** .

ADVANTAGE - Prevents pair of common sentence and code sentence to be known since count value is selected at random. Does not reduce intensity of code since top image data always differs even when same document is repeatedly transmitted. Does not change quantity of image data even when code key is changed.

Dwg.1/9

Title Terms: FACSIMILE; CODE; KEY; VARY; PART; CHANGE; SECRET; CODE; KEY; CODE; COMMUNICATE; ACCORD; RANDOM; NUMBER; **GENERATE** ; RANDOM; NUMBER; GENERATOR

Derwent Class: P85; W01; W02

International Patent Class (Main): H04L-009/00

International Patent Class (Additional): G09C-001/00; H04L-009/10; H04L-009/12; **H04N-001/44**

File Segment: EPI; EngPI

31/5/11 (Item 4 from file: 350)

DIALOG(R)File 350:Derwent WPIX

010358189 **Image available**

WPI Acc No: 1995-259503/199534

XRPX Acc No: N95-200077

Code communication method - decodes information received through predetermined communication circuit from call side terminal equipment based on reproduced **code key**

Patent Assignee: MITA IND CO LTD (MTAI)

Inventor: MORI T; NAKAMURA M; OYAMA M; SHIBATA K

Number of Countries: 002 Number of Patents: 002

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
JP 7162692	A	19950623	JP 93306764	A	19931207	199534	B
US 5574789	A	19961112	US 94341205	A	19941205	199651	

Priority Applications (No Type Date): JP 93306764 A 19931207

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
JP 7162692	A		7	H04N-001/44	
US 5574789	A		12	H04L-009/16	

Abstract (Basic): JP 7162692 A

The method involves transmission of the information enciphered through a predetermined communication circuit from the call side terminal equipment (1) to the called party terminal equipment. A **random number generator** (15) **generates** a **random number** sequence based on which a call side terminal equipment **produces** a code key using a control device (11). The NSS of option signal which contains **random number** sequence is used for generating code key and is transmitted through telephone circuit (3).

The encipherment / decipherment processing device (16) carries out encipherment of image data which is transmitted based on the code key. The code key is **reproduced** at the called party facsimile appts, based on the **random number** sequence. The received image is decoded based on the **reproduced** code key.

ADVANTAGE - Simplifies process by avoiding need for registering fixed code key in memory. Maintains secrecy of communication by transmitting **random number** sequence which is used for generating code key.

Dwg.2/6

Title Terms: CODE; COMMUNICATE; METHOD; DECODE; INFORMATION; RECEIVE; THROUGH; PREDETERMINED; COMMUNICATE; CIRCUIT; CALL; SIDE; TERMINAL; EQUIPMENT; BASED; **REPRODUCE** ; CODE; KEY

Derwent Class: P85; W01; W02

International Patent Class (Main): H04L-009/16; **H04N-001/44**

International Patent Class (Additional): G09C-001/06; H04L-009/06; H04L-009/14; **H04N-001/32**

File Segment: EPI; EngPI

31/5/12 (Item 5 from file: 350)

DIALOG(R)File 350:Derwent WPIX

008212551

WPI Acc No: 1990-099552/199013

XRPX Acc No: N90-076924

Information distribution **system for supplying encrypted packages - de-crypts and displays information selected by user reported by telephone**

Patent Assignee: CRYPTOLOGICS INT INC (CRYP-N); CRYPTOLOGICS INT IN (CRYP-N); INDATA CORP (INDA-N); SPRAGUE P J (SPRA-I)

Inventor: LIPSCOMB T H; MICHENER J R; PARKER J K; SPRAGUE P J

Number of Countries: 022 Number of Patents: 007

Patent Family:

Patent No	Kind	Date	Applicat No	Kind	Date	Week	
WO 9002382	A	19900308	WO 89US3474	A	19890814	199013	B
AU 8941882	A	19900323				199033	
EP 472521	A	19920304	EP 89909918	A	19890814	199210	
US 5247575	A	19930921	US 88232706	A	19880816	199339	
			US 89338275	A	19890414		

			US 89366150	A	19890614	
			US 92874991	A	19920424	
EP 472521	A4	19930630	EP 89909918	A	19890000	199526
EP 472521	B1	19980603	EP 89909918	A	19890814	199826
			WO 89US3474	A	19890814	
DE 68928694	E	19980709	DE 628694	A	19890814	199833
			EP 89909918	A	19890814	
			WO 89US3474	A	19890814	

Priority Applications (No Type Date): US 89366150 A 19890614; US 88232706 A 19880816; US 89338275 A 19890414; US 92874991 A 19920424
Cited Patents: US 4467424; US 4695880; US 4789863; 1.Jnl.Ref; US 4486853; WO 8802202; WO 8802960

Patent Details:

Patent No	Kind	Lan	Pg	Main IPC	Filing Notes
WO 9002382	A	E	61		
Designated States (National): AU BR DK FI HU JP KP KR NO SU					
Designated States (Regional): AT BE CH DE FR GB IT LU NL SE					
EP 472521	A				
Designated States (Regional): AT BE CH DE FR GB LI					
US 5247575	A		26	H04K-001/02	CIP of application US 88232706 CIP of application US 89338275 Cont of application US 89366150
EP 472521	B1	E		G06F-017/30	Based on patent WO 9002382
Designated States (Regional): AT BE CH DE FR GB LI					
DE 68928694	E			G06F-017/30	Based on patent EP 472521 Based on patent WO 9002382

Abstract (Basic): WO 9002382 A

The system provides information to a user, when the information corresponds to criteria individually selected by the user, and then charges the user only for the selected information this provided, encrypted information packages are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. The information packages selected by the user are decrypted and printed or displayed.

The charges for the information packages displayed are accumulated within the users apparatus and periodically reported to the systems cnetral accounting facility which issues encryption **keys** , which are changed periodically. If a new encryption **key** has not been issued the user will be unable to retrieve information from the system when the **key** is charged.

ADVANTAGE - Low cost information serives accessed by user in seamless manners. Min. telephone usage and central computing time.

Dwg.10/15

Title Terms: INFORMATION; **DISTRIBUTE** ; SYSTEM; SUPPLY; ENCRYPTION; PACKAGE ; DE; CRYPT; DISPLAY; INFORMATION; SELECT; USER; TELEPHONE
Derwent Class: T01
International Patent Class (Main): G06F-017/30; H04K-001/02
International Patent Class (Additional): G06F-015/28; G06K-005/00; H04B-017/00; **H04N-007/00**
File Segment: EPI